

REN-ISAC Activities and REN-ISAC / Internet2 Focus Group Results

Doug Pearson

Technical Director, REN-ISAC

Joint Techs, July 2005

How to Participate

To

- Join the vetted membership
- Receive REN-ISAC information product
- Participate in information sharing

<http://www.ren-isac.net/renisac-sec-l.html>

REN-ISAC Mission

- The REN-ISAC
 - is an integral part of higher education's strategy to improve network security through information collection, analysis, dissemination, early warning, and response; specifically designed to support the unique environment and needs of organizations connected to served higher education and research networks, and
 - supports efforts to protect the national cyber infrastructure by participating in the formal U.S. ISAC structure.

- In this presentation:
 - Quick outline of REN-ISAC Activities
 - Quick look at REN-ISAC information resources
 - Quick look at REN-ISAC information product
 - Summary of the results of an Internet2 & REN-ISAC Focus Group study

This isn't a full presentation about what the REN-ISAC is or does, if you'd like to see that:

<http://ren-isac.net/docs/ren-isac.pdf>

Activities

- Information products ...
- Incident response; broad-impact events and at request
- 24x7 Watch Desk; ren-isac@iu.edu, +1.317.278.6630
- Vetted membership / security contacts
- Tools (in conjunction with IU Advanced Network Mgmt Lab)
- Security infrastructures work in specific communities; e.g. grid security working groups
- Participate in mitigation communities
- Participate in other HE efforts; e.g Internet2/EDUCAUSE Computer & Network Security Task Force, SALSA
- Participate in other national activities, e.g. inter-ISAC, National Cyber Security Partnership, etc.

Information resources

- Network instrumentation
 - Abilene NetFlow
 - REN-ISAC Darknet
 - Abilene router ACL counters on common & threat ports
 - Global NOC operational monitoring systems
- Daily security status calls with ISACs and US-CERT
- Vetted network security collaborations, e.g. [XXXX]
- Backbone and member security and network engineers
- Vendors, e.g. monthly ISAC calls with vendors
- Security mailing lists, e.g. EDUCAUSE, FIRST, etc.
- Members – related to incidents on local networks

Information products

- Daily Weather Report
- Daily Darknet Reports
- Alerts
- Notifications
- Monitoring views

- We don't duplicate information flows provided by others, such as SANS ISC, US-CERT, etc. Rather, we provide unique product derived from our perspective and resources and provide value-add to existing information.
- Some information products are shared to the broad vetted membership, others to individual institutions involved in incidents. Privacy is important.

Daily Weather Reports

- Contain observations at aggregate levels of network threat traffic based on
 - Abilene NetFlow and
 - REN-ISAC Darknet (Abilene and commercial Internet)
 - Information and perspective from daily Inter-ISAC Cybersecurity Status calls
- Distributed to closed lists, including
 - REN-ISAC members and
 - Inter-ISAC plus DHS/US-CERT community
- Example
 1. highlights the Report structure

Daily Weather Report
Example #1: Report Structure

Date: Fri, 18 Mar 2005 10:07:23 -0500
To: renisac-sec-report-1@listserv.indiana.edu
From: Doug Pearson <dodpears@indiana.edu>
Subject: REN-ISAC Weather Report 2005.03.18

REN-ISAC Weather Report
2005.03.18
Please note the report sharing guidelines

CRITICAL NOTICES
=====

Nothing to report.

NEW WATCHES
=====

UDP/5093, SafeNet Sentinel License Manager, scanning yet, an exploit[*1] has been developed to exploit a buffer overflow vulnerability[*2]. The Metasploit SentinelLM service is installed with a wide selection of products. It seems particular popular with academic products."

[*1]
http://www.metasploit.com/projects/Framework/exploits.html#sentinel_lm7_overflow

[*2] <http://www.cirt.dk/advisories/cirt-30-advisory>
<http://secunia.com/advisories/14511>,
<http://www.kb.cert.org/vuls/id/108790>

FOLLOW-UPS
=====

Nothing to report.

Internet2 Abilene Aggregate Netflow[B] Traffic Analysis
=====

TCP/111 slightly elevated over the past 3 days
[http://www.ren-isac.net/monitoring/port-costa.cgi?tcp_data=111&socket=SUN_RPC_portmapper;vulnerabilities\[1\]](http://www.ren-isac.net/monitoring/port-costa.cgi?tcp_data=111&socket=SUN_RPC_portmapper;vulnerabilities[1])

TCP/135 returned to "normal" levels
[http://www.ren-isac.net/monitoring/port-costa.cgi?tcp_data=135&socket=MS_DCE_RPC_end-point_mapper;vulnerabilities\[2\]](http://www.ren-isac.net/monitoring/port-costa.cgi?tcp_data=135&socket=MS_DCE_RPC_end-point_mapper;vulnerabilities[2])

TCP/444 returned to "normal" levels
[http://www.ren-isac.net/monitoring/port-costa.cgi?tcp_data=444&socket=Simple_Network_Paging_Protocol;vulnerabilities\[3\]](http://www.ren-isac.net/monitoring/port-costa.cgi?tcp_data=444&socket=Simple_Network_Paging_Protocol;vulnerabilities[3])

CRITICAL NOTICES
contains high priority critical information; often this information is duplicated in separate Alerts.

NEW WATCHES contains reports of unusual new scanning activity such as scans against ports not seen in the past and substantial increases against common targets.

FOLLOW-UPS contains information regarding the continuing activity of reported earlier as Critical Notice or New Watch

NETFLOW TRAFFIC ANALYSIS contains observations of threat activity based on views of aggregate Abilene NetFlow

TCP/445 returned to "normal" levels
http://www.ren-isac.net/monitoring/port-costa.cgi?tcp_dst_445_packets
 MS Directory Services, aka SMB over IP, file shares; vulnerabilities[4]

TCP/3128 has dropped off somewhat, but continues to be elevated
http://www.ren-isac.net/monitoring/port-costa.cgi?tcp_dst_3128_packets
 Squid Cache proxy server; vulnerabilities[5]

REN-ISAC Darknet Monitor[C] Top Ports (Abilene & Commercial Internet)

port	count	percent change per period average			
		2-day	7-day	28-day	56-day
TCP/135	387164	34%	-62%	-63%	-63%
TCP/445	146890	-58%	-83%	-78%	-78%
TCP/1433	134470	43%	-79%	-79%	-79%
TCP/6101	133771	1036%	169%	73%	73%
TCP/1666	131528	184%	*	*	*
TCP/22	36322	-0%	-42%	-46%	-46%
TCP/139	35130	-70%	-88%	-82%	-82%
TCP/3127	18655	-42%	-67%	-62%	-62%
TCP/21	16213	89972%	-53%	-15%	-15%
TCP/1025	15896	-79%	-91%	-87%	-87%
TCP/4723	9380	-40%	-62%	29%	29%
TCP/80	7589	-65%	-87%	-90%	-90%
TCP/42	6362	-57%	-66%	-91%	-94%
TCP/4899	5654	-95%	-96%	-95%	-95%
TCP/4662	4552	-58%	-74%	-84%	-81%
UDP/137	127453	-64%	-62%	-63%	-58%
UDP/1434	113260	-52%	-71%	-68%	-63%
UDP/1026	6715	-78%	-82%	-84%	-79%
UDP/1027	6478	-54%	-68%	-82%	-78%
UDP/53	362	-52%	-63%	-76%	-72%

DARKNET MONITOR reports the top fifteen TCP and top five UDP scanned-for ports, and compares to averages over the past 2, 7, 28, and 56 days.

NOTE A: TCP/6101 no increase in sources

NOTE B: TCP/1666 predominately due to single source

NOTE C: TCP/21 predominately due to single source

REFERENCES
 =====

REFERENCES provide additional detail regarding vulnerabilities and exploits at TCP/UDP ports reported above

- [1] TCP/111 (SUN RPC portmapper)
 SANS security FAQ re port 111
<http://www.sans.org/resources/idfaq/blocking.php>
- [2] TCP/135 (MS DCE RPC end-point mapper)
 CERT Advisory CA-2003-23 RPCSS Vulnerabilities in Microsoft Windows
<http://www.cert.org/advisories/CA-2003-23.html>
 CERT Advisory CA-2003-20 W32/Blaster worm

<http://www.cert.org/advisories/CA-2003-20.html>
Symantec W32.Welchia.Worm

<http://securityresponse.symantec.com/avcenter/venc/data/w32.welchia.worm.html>

[3] TCP/444 (Simple Network Paging Protocol)
A vulnerability exists in SUN RaQ server appliances running Security Hardening Package.
CERT Advisory CA-2002-35 Vulnerability in RaQ Server Appliances
<http://www.cert.org/advisories/CA-2002-35.html>

[4] TCP/445 (MS Directory Services, aka SMB over IP, file shares; vulnerabilities)
CERT Advisory CA-2003-08 Increased Activity Targeting Windows Shares
<http://www.cert.org/advisories/CA-2003-08.html>
CERT Advisory CA-2003-23 RPCSS Vulnerabilities in Microsoft Windows
<http://www.cert.org/advisories/CA-2003-23.html>

[5] TCP/3128 (Squid Cache proxy server)
Scanning on TCP/3128 may be searching for open proxies. The Mydoom backdoor normally listens on 3127, but will use next available in the range 3128-3199 if ports are already in use. Mydoom acts as a SOCKS proxy and supports backdoor commands and remote execution. Various other trojans use 3128 including Reverse WWW Tunnel Backdoor, RingZero, MastersParadise, W32.HLLW.Deadhat.

[A] This report can be shared within ~~closed~~ communities of cyber security practitioners. It must NOT be shared publicly.

[B] Abilene netflow graphs for a number of common and threat vector ports can be seen at <http://ren-isac.net/monitoring.cgi>.

[C] Data collected using the REN-ISAC Internet Motion Sensor deployment, <http://ims.eecs.umich.edu/>

Research and Education Networking ISAC
24x7 Watch Desk: +1(317)278-6630
ren-isac@iu.edu
<http://www.ren-isac.net>

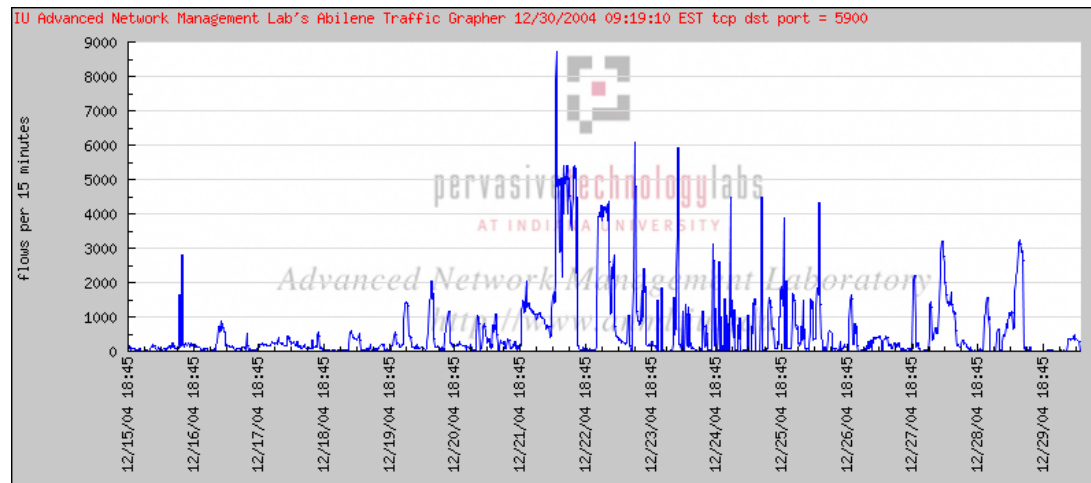
-o0o-

Daily Darknet Reports

- The REN-ISAC Darknet is a deployment of the University of Michigan Internet Motion Sensor project.
- The Darknet contains a large block of dark IPv4 address space routed to a collector that records traffic inbound to the address space – it hears automated and manual scanning from malware (e.g. bots, worms) and perps.
- REN-ISAC parses the information according to source member institutions, and sends reports of sources seen to the respective institution.
- Institutions remediate the affected systems
- Currently monitoring 41 Internet2 sites; growing
- Example: Indiana University

Alerts

- Alerts contain critical actionable information alerting the broad membership to new or increasing network-based threat.
- Alerts are sent as required, to: REN-ISAC members, and as appropriate to other network security groups.
- Example: Dec 2004, increased TCP/5900; scanning for trojans with VNC backdoors?



Notifications

- Notifications contain actionable information about active network-based threat or incident involving a specific institution.
- Notifications are sent to the involved (source and victim) institutions.
- Typically contain identification of specific hosts.
- Example:
 - March 2005; Keylogger botnet involving 46 EDU institutions (Internet2 and non-Internet2)

Monitoring

- Abilene NetFlow
- Publicly available reports of Abilene traffic stats for common and threat vector ports, published to the REN-ISAC web pages
 - <http://www.ren-isac.net/monitoring.cgi>
- Arbor PeakFlow DDOS
- Darknet

Abilene Traffic by Port



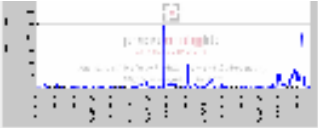
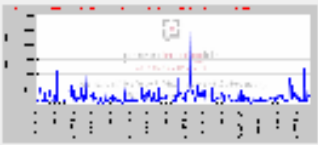
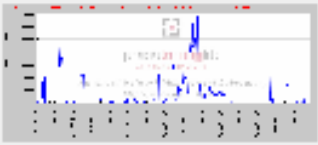

[REN-ISAC Home](#) >> [Monitoring](#)

- About
- Contacts
- Members
- Register
- Library
- Monitoring
- Watch Desk
- Request Info
- Security News
- Policies
- Home

These port traffic graphs are generated from aggregate Abilene netflow data, sampled at 1:100.

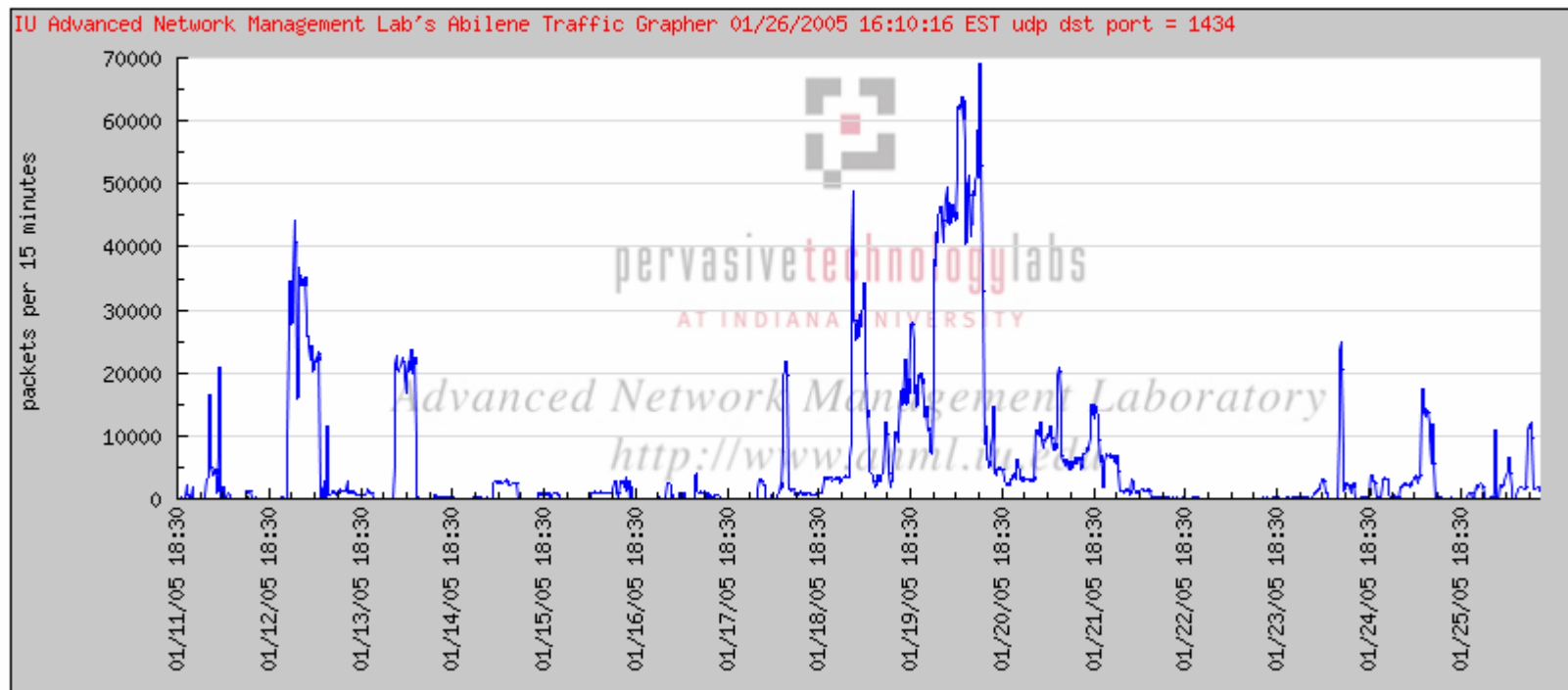
port	protocol	service	monitoring links	best practice	vulnerability / exploit / notes
20	tcp	ftp-data		.	
21	tcp	ftp		.	
22	tcp	ssh		.	
23	tcp	telnet		.	
25	tcp	smtp		.	CA-2003-07 : Remote Buffer Overflow in Sendmail CA-2003-12 : Buffer Overflow in Sendmail CA-2003-25 : Buffer Overflow in Sendmail
42	tcp	WINS server replication protocol		.	US-CERT VU#145134 : WINS Vulnerability MS04-045
42	udp	WINS		.	US-CERT VU#145134 : WINS Vulnerability
53	tcp	dns		.	CA-2002-31 : Multiple Vulnerabilities in BIND
53	udp	dns		.	CA-2002-31 : Multiple Vulnerabilities in BIND

Abilene Traffic by Port

1433	udp	.		.	Microsoft-SQL-Server
1434	tcp	Microsoft-SQL-Monitor		.	CA-2003-04 : MS-SQL Server Worm
1434	udp	Microsoft-SQL-Monitor		.	CA-2003-04 : MS-SQL Server Worm
					

Abilene Traffic by Port

[REN-ISAC Home](#) > > [Monitoring](#) > > [udp_dst_1434_packets](#)



Focus Groups

- Goal: Determine what the REN-ISAC & Internet2 can do to help security and network practitioners better defend their local environments.
- Two sessions: June 24 and 30; 9 universities, mostly Carnegie classification “Doctoral/Research Universities – Extensive”, i.e. medium-to-large research universities.
- Method:
 - small groups of interviewees (< 6 per session)
 - prior to FG, each interviewee identified top 5 issues
 - single interviewer
 - list of questions, but free to roam; 1.5 hour session
 - group of experts communicated to interviewer via IM, prompting additional/exploratory questioning

FG: How do you identify misbehaving hosts?

- high: reliance on multiple methods, e.g. "use three tiers – active scanning, passive detection with netflow, and passive signature-based detection"
- high: receive notifications and/or pull information from outside sources, including other EDUs, DShield, REN-ISAC darknet reports, etc.
 - med: initially verify reports locally, e.g. netflow, argus, etc., but when establish consistent veracity of source then take reports as gospel
 - high: find the reports very useful, and do follow-up
- high: local abuse@[org.edu] contact point is actively monitored

FG: How do you identify misbehaving hosts?

- high: use netflow to identify misbehaving hosts
 - lots of local-custom scripts (most often used in conjunction with flow-tools)
 - on the fly inspection and stored-look-at-later
 - periodically run scripts looking for known indicators, such as scanning, connections to known bad internal and external hosts, top talkers on given IP ports, etc.
 - low: look for bandwidth per host anomalies
 - low: concern regarding sampling due to traffic level (led one to move to a commercial flow analysis system); other comments - still very useful even if sampling
 - mix of what's being looked at: more oriented to flows at the border than in the core; more oriented to outbound than inbound

FG: How do you identify misbehaving hosts?

- high: vulnerability and port scanning
 - vulnerability scanning using (in order of common use) (1) Nessus, (2) ISS; (3) Retina; some sites use more than one
 - and Nmap for port scanning
 - a mix of central and distributed (departmental) scanning
 - high: movement to centralize scanning resources and tools make the central scanners accessible to the departments and/or users
 - low: packaged scanning tools (i.e. on CD-ROM, etc.) provided to departments/system administrators
 - zero: policies that preclude departments from deploying their own scanners in their domains

FG: How do you identify misbehaving hosts?

- high: vulnerability and port scanning (CONTINUED)
 - mix of approaches
 - scan only when new a threat comes out
 - occasionally scan all hosts all ports (very time consuming) plus more frequent scans at known bad ports
 - look for banners, e.g. 220 messages (SMTP servers), at unusual port numbers
 - scanning becoming less useful as host-based firewalls come online; leading to more use of passive detection, but still useful for detecting backdoors
 - low: scan wireless and modem address space
 - med-low: automated scanning; most of those who are not automated are heading in that direction

FG: How do you identify misbehaving hosts?

- high: vulnerability and port scanning (CONTINUED)
 - med: tying scanning into network registration systems – with side benefit to solve the DHCP-created IP address-to-owner disconnect problem for scan reporting

FG: How do you identify misbehaving hosts?

- med-high: use of Snort
 - look for suspicious traffic patterns, loud talkers, hosts walking the address space, etc.
 - some paring-down of out-of-box rule sets in order to reduce false positives
 - issue with performance, e.g. capability to deal with network bandwidth, ability to keep up with scanning detection and packet inspection, high peaks of worm scanning, etc., leads some to:
 - multiple/distributed Snorts
 - move scanning detection to darknet, save Snort for packet inspection tasks
 - some to think about large commercial IDS/IPS
 - some use of BASE (Basic Analysis and Security Engine)

FG: How do you identify misbehaving hosts?

- low: use of commercial IDS/IPS
 - detect packet signatures, port-scanners, hosts with large number of session opens, etc.
 - high: concern regarding interfering with research-oriented non-standard traffic (mitigation: tune to block only the things that are well understood)
 - high: concern regarding ability to meet bandwidth requirements
 - med: concern regarding blocking of legitimate traffic at non-standard ports
 - comment: lots of human resource currently invested in getting good use out of Snort, open source tools, etc., a magic IPS box should reduce the resource requirements considerably, but haven't found the magic box yet

FG: How do you identify misbehaving hosts?

- med: system administrators inspect system logs for malicious activity
- med: inspect DNS traffic; use of DNS query logs
- low: router log analysis
- low: bandwidth reports
- low: darknet, but med: interest in darknet
- low: QRadar
- low: Argus
- low: local users/system administrators identifying miscreant IRC activity

FG: How do you identify misbehaving hosts?

- low: locally-developed web spiders looking for institution or institution data-identifying information
- low: automation to take notifications from sources (local sensors, outside reporters, etc.) directly into back-end system to generate alerts to LAN administrators or incident response teams

FG: Incident Response / Investigation

- high: capability for incident responders to quickly kill ports (some in direct control, others via quick process with NOC)
- low: automatic blocking of ports/hosts (i.e. without a person in the middle)
- med-high: when protected data is involved the central security office gets involved in investigation, forensics, etc.
 - low: policies that require reporting of incidents to the central security office; but most receive the reports anyway; and many have policies in the works
 - in some cases driven by state laws requiring notification of personal data compromise
 - a few notable exceptions
 - "We usually don't - we keep data from flows and logs, and the departments handle the investigation of incidents themselves", and

FG: Incident Response / Investigation

- a few notable exceptions (CONTINUED)
 - "Forensic response is a costly resource and is not encouraged. It's not policy to quiz people about data on the machine. Sometimes that's obvious and then the response takes a different path."
- med: use of netflow to identify all flows for affected host(s)
- med: forensics capability
 - med-low: formal forensics training
 - low: certified forensics personnel, e.g. GCFA
 - med: training expected soon
- low: toolsets provided to departments/system administrators for system recovery and forensics; e.g. Knoppix/Helix, etc.

FG: Prevention

- med: blackhole known external sources of malware, hacking, etc.
 - typically only in extreme cases
 - typically don't do it just from external reports but confirm it on the local network
 - to trust external lists would need to have a really good definition of how/why hosts get on the list and how they get off; along with information about how critical a particular entry is; even then, many would still locally confirm the activity
 - mixed opinions within the institutions themselves

FG: Internal Information Sharing

- med: institutional private mailing lists where security matters, including tools and methods are discussed
- med: incidents/compromises discovered at departments are reported to a central organization

FG: External Information Sharing

- high: local submissions of captured codes to antivirus vendors
- high: try to notify other EDUs when have information regarding misbehaving machines, but
 - difficult to do - proper contact, time, methods, etc.
 - difficult because the number of hosts involved is typically very large
- the [anticipated] REN-ISAC registry would be really helpful
- if know clueful contacts, would probably report more
- UNISOG and REN-ISAC are good resources
- abuse@[org.edu] contact points usually work

FG: Data Retention Policies

- low: official policies regarding data retention
- high: flow data kept for 14-90 days; low: keep forever
- high: system logs, authentication records, mail records, etc. kept 6 months -> forever
- high: don't store payloads (only for the duration of an investigation)

FG: Tools

- high: netflow
- high: custom in-house developed scripts for netflow, mostly in conjunction with flow-tools
- high: Nessus preferred over ISS, etc.
 - can look at the vulnerability checks and understand definitively what they're going to do and how they're doing it
 - easier to customize scripts to local environment
 - more flexible, e.g. for single vulnerability checks
 - community support is strong
 - low: ISS requires administrator rights on remote machines for some checks, and "we don't have and never will"

FG: Tools

- high: Nessus preferred over ISS, etc. (CONTINUED)
 - on the negative side, Nessus is more difficult for the non-professionals (i.e. departments, end-system administrators) to interpret results than ISS
- high: Nmap
- high: willingness to share locally developed tools
 - tools are discussed and shared at UNISOG, international ISP security communities, in regional security groups and conferences
 - but want to keep the sharing limited to white hats

FG: Other Areas

- Talked about the following in the FG, but not presented here due to time. Will be included in follow-on reports:
- HOST/NETWORK REGISTRATION
- WIRELESS
- VPNs

FG: Would like to see the REN-ISAC do...

- help organizations to take a better and more strategic approach to network intelligence that's gathered, e.g. what needs to be collected, what the purposes are, where should the information go, policy for handling, retention, etc.
- methods (including standards and policies) to share observations of misbehaving hosts that are external to the local institution
- serve as an anonymization point for information sharing, e.g. "I'm seeing this sort of behavior" messages, Snort rules, etc., accepted from a trusted contact and distributed anonymously to the trusted community
- serve as a trusted meeting point for peers, i.e. "I know that if they're here that they've been vetted according to XYZ" meeting point

FG: Would like to see the REN-ISAC do...

- reach out beyond the higher-ed community – where they can help us and we can help them
- facilitate communications - make it easy for institutions to find each other and find the right contacts, quickly
- tool repository
- recommendations regarding best practices for border filtering – what to filter, what not to filter, and why; such community consensus guidelines would provide authority and backing to recommendations made to local decision makers
- standardization and/or sharing of information around the use of flow tools
- security contact information

FG: Would like to see the REN-ISAC do...

- rankings of the amount of misbehavior seen from institutions (while not making the rankings public)
- coordinate alliance to acquire commercial products, e.g. Arbor for gigapops, etc.
- information regarding state and local laws that bind institutions, e.g. legal precedents regarding log retention, etc.
- DShield-like service
- regular security workshop similar to EDUCAUSE, Jt. Techs
- taxonomy of tools and pointers to people that have them
- current security best practices guides ignore the open end-to-end concept, need credible best practices for security implementations that respect end-to-end openness

FG: Would like to see the REN-ISAC do...

- organize funding and grants for information sharing activities among the institutions

FG: Path Forward

Some of the preceding suggestions match very well to the REN-ISAC mission and some match better to other groups, such as EDUCAUSE Effective Practices, etc.

REN-ISAC will work Internet2, EDUCAUSE, SALSA, and with its [to-be-formed] Technical and Executive Advisory Groups to determine paths forward on the results of the FGs.

How to Participate

To

- Join the vetted membership
- Receive REN-ISAC information product
- Participate in information sharing

<http://www.ren-isac.net/renisac-sec-l.html>

Doug Pearson <dodpears@iu.edu>

PGP: http://mypage.iu.edu/~dodpears/dodpears_pubkey.asc

Research and Education Networking ISAC

24x7 Watch Desk: +1(317)278-6630

ren-isac@iu.edu

<http://www.ren-isac.net>